UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,683	06/20/2003	Erik Olson	13768.373	4994

47973 7590 12/15/2006

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/600,683	OLSON ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 – 12, 14 – 22, 24 – 29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 – 12, 14 – 22, 24 – 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/21/06 has been entered.

Claims 1 – 12, 14 – 22, 24 – 29 are pending.

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 – 12, 14 – 22, 24 – 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, claims 1, 8, and 18, each comprise the limitation (or essentially similar), *"requesting that the user computer resubmit the request"*. However, the examiner notes that if a submitted request is a malicious request, then according to the applicant's original disclosure, the user computer is requested to send a non-malicious request – not the malicious request. Thus, this limitation is ambiguous as the claims suggest that a malicious request is being resubmitted.

Depending claims are rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 12, 14 – 22, 24 – 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over CERT CC, "CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests" (CERT-Advisory) in view of CERT CC, "Understanding Malicious Content Mitigation for Web Developers" (CERT) in view of Wheeler, Secure Programming for Linux and Unix HOWTO.

Regarding claim 8, CERT-Advisory discloses:

receiving an HTTP request at a server computer, wherein the HTTP request includes input data that was not generated by the server computer (CERT-Advisory, page 1, Systems Affected, Overview; page 2, pars. 2-4).

CERT-Advisory discloses, in general, that the Server site attempts to filter the incoming HTTP request according to the criteria of removing dangerous meta-characters, so as to prevent their sites from being attacked, "abused", by malicious data or a cross-site scripting attack (CERT-Advisory, page 5, Solutions for Web Page Developers and Web Site Administrators). While one of ordinary skill in the art would rightly and easily conclude from the context of CERT-Advisory that the incoming meta-characters being filtered are being evaluated against known scripting constructs or characters, CERT-Advisory does not *explicitly* say the evaluation is to determine *if the input data includes a script construct, wherein the script construct indicates that HTTP request is part of a cross-site scripting attack.* Instead, CERT-Advisory directs the readers' attention to the detailed solution (found in CERT) for preventing cross-site scripting attacks in response to receiving HTTP requests comprising malicious scripts.

CERT discloses the specifics for mitigating cross-site scripting attacks by evaluating the incoming data requests to determine the presences of dangerous meta-characters, indicating the presence of malicious scripts (CERT, page 1, par. 1, Problem Summary, pars. 2-3; page 2, Mitigation Summary; page 3, Identifying the Special Characters; page 4, Filtering Dynamic Content). CERT, thus clearly demonstrates that the filtering of input data for dangerous meta-characters is an evaluation of the presence of malicious script constructs.

It would have been obvious to one of ordinary skill in the art to combine the teachings of CERT, for evaluating input data for script constructs - in addition to other specific teachings of CERT for mitigating cross-site scripting attacks - with the system of CERT-Advisory. This would have been obvious because CERT-Advisory explicitly says to include the reference of CERT so as to successfully mitigate cross-site scripting attacks (CERT-Advisory, page 5, par. 6).

The combination of CERT-Advisory and CERT discloses *refusing to dynamically render a response to the HTTP request if the input data includes a script construct* (Examiner Notes: The applicant's originally disclose that a server, in response to the malicious request will serve an informative response to the user indicating an error and requesting that the user submit a non malicious request. Thus, the examiner interprets the applicant's limitation *refusing to dynamically render a response* to mean *refusing to execute the HTTP request*, as the applicant have originally disclosed.) (CERT-Advisory, pg. 1, "Overview"; pg. 2, "Malicious code sent inadvertently by a client for itself"; CERT, pg. 1, par. 1; pg. 2-4, "Mitigation Summary"). Herein, prior art discloses that if the input data includes a script construct, refusing to execute HTTP request and thereby preventing the cross-site scripting attack if the input data includes a script construct. Malicious HTTP requests are not executed. Furthermore, the combination discloses filtering and encoding to remove malicious scripts and data for every HTTP request.

The combination does not disclose *informing the user that a marker of active content has been discovered in the request and requesting that the user computer*

resubmit the request and subsequently serving a response to a request resubmitted by the user computer.

Wheeler, in response to the problem of cross-site scripting attacks and building upon the prior art teachings of CERT (Wheeler, 4.10, 6.15, 6.15.1 – 6.15.2.1, 8.5), teaches that a system in practice may forbid markers of active content and send informative error messages to users who include them in requests. A system could notify the user of ways to correct such issues (Wheeler, 4.11.6, par. 2; 4.11.1; 4.11.3, par. 5; 4.12, par. 5).

It would have been obvious to one of ordinary skill in the art to employ the teachings of Wheeler along with the teachings of the combination of CERT and CERT-Advisory. This would have been obvious because one of ordinary skill in the art would have been motivated by the explicit suggestions found within the prior art when practically implementing a solution to mitigate malicious scripting attacks.

Regarding claim 9, the combination disclose:

at least one of: receiving a query string that includes at least one query string variable; receiving a cookie; receiving one or more headers in the HTTP request; and receiving one or more form fields (CERT-Advisory, page 2, pars. 2-5; CERT, page 2, Mitigation Summary).

Regarding claim 10, the combination disclose:

at least one of: searching the HTTP request for one or more character combinations that correspond to a script construct; searching the HTTP request for an event that includes a script construct; searching server variables that derive input data from another source; and searching the HTTP request for an expression that includes a script construct (CERT, page 3, Identifying the Special Characters; page 4, Filtering Dynamic Content).

Regarding claim 11, the combination disclose:

searching the input data for a script construct (CERT, page 3, Identifying the Special Characters; page 4, Filtering Dynamic Content).

Regarding claim 12, the combination disclose:

searching for patterns associated with scripts (CERT, page 3, Identifying the Special Characters; page 4, Filtering Dynamic Content).

Regarding claim 14, the combination disclose:

wherein preventing the cross-site scripting attack if the input data includes a script construct further comprises logging an event at the server computer (Wheeler, 8.1; 10.9; 10.11). Herein, the combination disclose that a server generates a detailed log of events regarding system successes and failures, in addition to sending a response back to the user regarding the event – such as why there was a failure.

Regarding claim 15, the combination of CERT-Advisory, CERT, Hidalgo, and Fielding disclose:

encoding the user input including the script construct to render the script inert (CERT-Advisory, page 2, par. 1; page 5, pars. 3-6; CERT, page 3, Identifying the Special Characters; page 4, par. 2).

Regarding claim 16, the combination of CERT-Advisory, CERT, Hidalgo, and Fielding disclose:

evaluating the HTTP request to determine in the input data includes a marker of active content (CERT, page 2, Mitigation Summary – particularly steps 2 and 4; page 3, Identifying the Special Characters).

Regarding claim 17, the combination of CERT-Advisory, CERT, Hidalgo, and Fielding disclose:

determining if the marker of active content is within a particular element, wherein the marker of active content is harmful only when rendered within the particular element (CERT, page 2, Mitigation Summary – particularly steps 2 and 4 (identifying special characters, filtering specific characters in dynamic elements; page 3, Identifying the Special Characters).

Regarding claims 1 – 3, 5 – 7, 18 – 22, 24, and 25, they are method and method embodied on computer readable medium claims corresponding to the system claims 1 – 17, and they are rejected, at least, for the same reasons.

Regarding claim 4, the combination disclose: *evaluating only a portion of the request that includes the data derived from an outside source* (CERT, page 2, Mitigation Summary; Wheeler, sect. 4, par. 1, 12). The combination of CERT-Advisory and CERT discloses the need to evaluate data comprising untrusted input that could be transmitted in an HTTP request.

Regarding claim 26, the combination enables:

wherein determining if the request from the user computer includes a marker of active content comprises evaluating only user input fields of the request (CERT, page 2, Mitigation Summary; Wheeler, sect. 4, par. 1, 12). The combination of CERT-Advisory and CERT discloses the need to only evaluate data comprising untrusted input that could be transmitted in an HTTP request. Thus, it is obvious that if the only untrusted input of a request comprises user input fields, then the combination would evaluate the user input fields.

Regarding claim 27, the combination discloses *maintaining a list of markers of active content* (Cert, pg. 4, 5). The combination does not disclose *inactivating markers in the list of markers*. However, the notion of updating/modifying a list used in

performing security checks was known and would have been obvious to one of ordinary skill in the art. One of ordinary skill in the art would have been motivated to modify the list [such as by "inactivating" list elements] as it would enable for a more flexible or customizable system. For evidentiary teachings of customizable systems that prevent cross-side scripting attacks, the applicant may refer to any of the cited prior art, including Scott et al., "Abstracting Application-Level Web Security" (pg 1:col. 2:par. 3; pg. 3:col. 2:par. 1; pg. 6:col. 1:par. 1) or Sirer et al., "An Access Control Language for Web Services (pg. 1:col. 2:par. 1; pg. 4:col. 2:par. 2).

Regarding claim 28, the combination discloses:

wherein evaluating the HTTP request to determine if the input data includes a script construct comprises evaluating the HTTP request for an event (Wheeler, sect. 4.11.3, box of attack types). Herein, the combination teaches to test for events, such as 'onmousover' events. It does not disclose onclick events, however, one of ordinary skill in the art would have recognized that an 'onclick' events similarly introduce scripts such as 'onmouseover' events (applicant may refer to evidence such as W3C Recommendation, "Scripts") and would have been motivated to test for malicious constructs.

Regarding claim 29, the combination discloses:

wherein evaluating the HTTP request to determine if the input data includes a script construct comprises evaluating the HTTP request for an element size expression (Wheeler, sect. 4.11.3, box of attack types).

Response to Arguments

Applicant's arguments filed 9/21/06 have been fully considered but they are not persuasive.

Applicants argue primarily that:

(i) *For example, among other things, CERT I, CERT II and Hidalgo fail to disclose or suggest refraining from serving a response to the request if the request includes the marker of active content, and instead serving a response only to a request resubmitted by the user computer, as recited in combination with the other claim elements.*

In fact, and in direct contrast to the above claims, CERT I and CERT II specifically teach that rather than aborting the request so as to refrain from serving a response, the request is processed and a response is in fact returned. (Remarks, pg. 13).

First, the examiner notes, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re*

Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Second, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *serving a response only to a request resubmitted by the user computer*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Third, in light of the applicant's allegation of a "direct contrast" between the prior art and the applicant's invention, the examiner points out that "returning a response" to the user computer upon submission of a malicious request, is in fact the prior disclosure of the applicant (ex. see Specification, previously claimed 8). As does the applicant, prior art discloses returning a response upon reception of a malicious request, wherein at no time are malicious requests executed.

Applicant's arguments with respect to claims 1 - 29 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams
AU: 2137
JW

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER